ANDROID. АНАЛИЗ ПРИЛОЖЕНИЙ ДЛЯ ШИФРОВАНИЯ

Д. О. Спирин
(Тюмень, ТюмГУ, DenisSpirin92@Gmail.com)

Введение

Согласно прогнозу, опубликованному компанией Cisco, число мобильных устройств, подключенных к Сети, скоро превысит население земли. На текущий момент более 6 млрд человек пользуются мобильными телефонами [4]. Смартфоны, представляя лишь 18 % мобильных устройств, пропускают 92 % мирового мобильного трафика. Мобильные телефоны давно представляют собой полноценные узлы Сети, но, что удивительно, не воспринимаются как таковые. В бытовом сознании смартфон – это лишь телефон, не способный на серьезные операции.

Между тем современное устройство может находиться включенным 24 часа 7 дней в неделю через один или несколько сетевых интерфейсов, синхронизироваться со стационарными компьютерами или облачными сервисами, проходить аутентификацию в различных интернет-сервисах, использовать геопозиционирование, получать доступ к корпоративными ресурсам извне, а также хранить записи, фотографии и документы различной степени важности. Поток информации, проходящей через мобильные устройства, достигает внушительных объемов, и его нужно как-то защищать. Эта проблема уже неоднократно поднималась в кругах исследователей [1; 2; 3].

Защита мобильных устройств, особенно в компаниях с политикой BYOD, является серьезной проблемой. В последнее время стали набирать популярность приложения, предоставляющие услуги шифрования и скрытия данных. Однако способность данных приложений предоставить достаточную защиту данных остается под вопросом. В этой работе будут резюмированы данные, полученные после анализа ряда подобных приложений для наиболее популярной мобильной платформы Android.

Модель угроз нарушителя

Мобильные устройства подвержены разнообразным рискам. Каждую минуту в США крадут 113 телефонов, а в Лондоне каждый день – 314 телефонов, 120 тыс. телефонов забывают в такси в Чикаго. В январе 2013 г. у израильской чиновницы похитили телефон с секретными сведениями [5]. Кроме того, серьезную угрозу представляет вредоносное ПО (рис. 1).

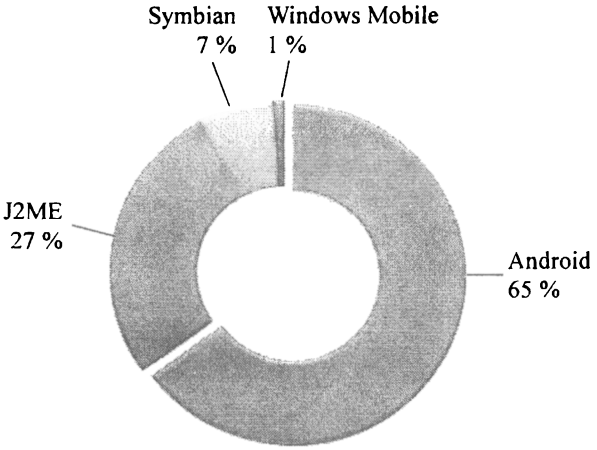

Рис. 1. Распределение модификаций мобильных вредоносных программ по платформам в 2011 г. по данным Лаборатории Касперского

Рис. 2. Количество обнаруженных модификаций вредоносного программного обеспечения для Android OS

На рис. 1, 2 видно, что создание вредоносного ПО для платформы Android не только привлекательно для злоумышленников, но и успешно им удается [6; 7]. Проблему в данном случае усугубляет низкий контроль качества в Google Play, а именно – по жалобам пользователей. Злоумышленник может выпускать перепакованные копии известных продуктов с вредоносными вставками или добавлять уязвимости в обновлениях. И в довершение в этому рядовой пользователь, не глядя, предоставляет приложениям неограниченные полномочия, часто в системе, работающей из-под корневой записи.

Злоумышленник, используя описанные выше уязвимости, может получить физический доступ к телефону или же дистанционно атаковать OS. Основными его целями после этого станут заметки, файлы, а также интернет-сервисы с сохраненными паролями.

Обзор приложений

В Google Play были выбраны приложения, которые:

1. Бесплатны.
2. Были скачаны не менее 100 тыс. раз.
3. Содержат ключевые слова: encrypt, protect files, protect images.

В качестве методов исследования использовались:

1. Анализ внешнего носителя.
2. Анализ внутреннего носителя.
3. Тестовые данные.

Общее число установок: более 12 млн.

Приложения:

1. Safe Notes установок 500 000–1 000 000.
2. OI Safe установок 100 000–500 000.
3. Password Safe lite установок 100 000–500 000.
4. Secret Safe lite установок 100 000–500 000.
5. Keeper установок 1 000 000–5 000 000.
6. B-folders password manager установок 100 000–500 000.

Поскольку приложения содержат повторяющиеся ошибки, то чтобы не останавливаться на каждой из них в отдельности, перейдем к повторяющимся уязвимостям:

1. Фиксированные ключ.
2. Слабые алгоритмы хеширования.

3. Применения обычных хешей вместо Key derivation functio.
4. Формирование ключа из непосредственно пароля.
5. Слабые режимы шифрования.
6. Хранение данных в XML-файлах.

Заключение

В то время как Google Play предлагает огромное количество приложений, обещающих надежное шифрование, безопасность, имеющих наивысший рейтинг и оценку в 5 звезд, их функциональность сомнительна. Злоумышленник, сумевший получить доступ к устройству тем или иным способом, без особого труда обойдет средства «защиты», используемые в этих приложениях. Реклама подобных продуктов создает опасное заблуждение о безопасном хранении данных.

В силу отсутствия каких-либо сертифицированных средств можно сделать вывод, что защита важных данных на мобильных устройствах под управлением Android невозможна, и единственным выходом является неиспользование мобильных устройств для хранения подобной информации.

Библиографические ссылки

1. *Ванг Й.*, *Стрефф К.*, *Раман С.* Проблемы безопасности смартфонов // Открытые системы. 2013. № 01 [Электронный ресурс]. URL: http://www.osp.ru/os/2013/01/13033981/ (дата обращения: 03.10.13).

2. *Fahl S.*, *Harbach M.*, *Muders T.*, *Baumgärtner L.*, *Freisleben B.*, *Smith M.* Why eve and mallory love android: an analysis of android SSL // ACM Digital Library. 2011 [Электронный ресурс]. URL: http://dl.acm.org/citation.cfm?id=2382205 (in)sec (дата обращения: 03.10.13).

3. *Vidas T.*, *Votipka D.*, *Christin N.* All your droid are belong to us: a survey of current android attacks // ACM Digital Library. 2012 [Электронный ресурс]. URL: http://dl.acm.org/citation.cfm?id=2028062&CFID=370234942&CFTOKEN=14577168 (дата обращения: 03.10.13).

4. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012–2017 [Электронный ресурс]. URL: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html (дата обращения: 03.10.13).

5. Глобальный еврейский Online Центр [Электронный ресурс]. URL: http://www.jewish.ru/news/israel/2013/01/news994314013.php (дата обращения: 3.10.13)

6. *Безмалый В.* Новое время – новые угрозы // Windows IT Pro/RE: проф. изд., посв. вопросам работы с продуктами семейства Windows и технологиям компании Microsoft. 2012 [Электронный ресурс]. URL: http://www.osp.ru/win2000/2012/08/13033288/ (дата обращения: 03.10.13).

7. *Ледовской В.* Android под прицелом. Беззубая свобода // Anti-Malware.ru – первый в России независимый информационно-аналитический центр, полностью посвященный информационной безопасности. 2012 [Электронный ресурс]. URL: http://www.anti-malware.ru/analytics/Android_under_sight/ (дата обращения: 03.10.13).

УЯЗВИМОСТЬ И ЗАЩИТА АЛГОРИТМА ДИФФИ – ХЕЛЛМАНА

Е. О. Федюшина, М. А. Балашов
(Екатеринбург, УрГУПС, eleno4ka45@mail.ru)

Безопасность систем шифрования зависит от конфиденциальности ключа, используемого в алгоритме шифрования, а не от хранения в тайне самого алгоритма. Многие алгоритмы шифрования общедоступны и были хорошо проверены благодаря этому. Цель данной работы – изучить алгоритм обмена ключей Диффи – Хеллмана как пример шифрования с открытым ключом, выявить его уязвимость и найти способ ее устранения.

Алгоритм Диффи – Хеллмана – алгоритм, позволяющий двум сторонам получить общий секретный ключ, используя незащищенный от прослушивания, но защищенный от подмены канал связи. Этот ключ может быть использован для шифрования дальнейшего обмена с помощью алгоритма симметричного шифрования.

Система Диффи – Хеллмана разрабатывалась для решения проблемы распространения ключей при использовании систем шифрования с секретными ключами. Идея заключалась в том, чтобы применять безопасный метод согласования секретного ключа без передачи ключа каким-либо другим способом. Следовательно, необходи-